2022 年度 卒業研究発表 梗概

電気学科

| 学籍番号<br>氏　名 | V19131　樋口 葵 | 指導教員 | 藤枝 直輝 |
|---|---|---|---|
| 題　目 | SCR1 プロセッサに対する<br>命令レジスタファイルによる命令難読化の実装 | | |

## 1　背景

ソフトウェアを分析、盗用、改ざんといった攻撃に対して強くすること、すなわち耐タンパー性を高めることは重要である。コンピュータやインターネットが普及した結果、コンピュータのソフトウェアを対象とした攻撃も日々発生している。また、その件数は年々増加してきている。ソフトウェアには個人や企業のノウハウなどが詰まっており、これを攻撃から守ることは、知的財産を守ることにつながる。攻撃の 1 つとして、プログラム内容の解析、すなわちリバースエンジニアリングの悪用が挙げられる。

プログラムの難読化の方法として、IRF（命令レジスタファイル）による命令難読化が挙げられる [1]。IRF とは命令を格納した小さなメモリであり、もともとプロセッサの性能向上を目的として提案された。特定の命令を、IRF を参照する命令“IRF 命令”に置き換え、この命令がフェッチされたら IRF を参照し元の命令に置き換える。IRF の内容がわからない限り、元の命令の類推は困難となる。

## 2　先行研究と研究目的

米澤らは RISC-V 命令セットをもつ CVA6 プロセッサに対する、IRF による命令難読化について検討した [2]。32 ビットの通常命令と 16 ビットの短縮命令が混在する中、IRF による命令置き換えが可能であることを示した。しかし、搭載した IRF は、1 つの短縮命令しか置き換えできないプロトタイプであった。

本研究の目的は RISC-V 命令セットを持つ SCR1 プロセッサにおいて、複数の、かつ短縮命令と通常命令の両方に対応した IRF を実装する。また、実用性向上のため、IRF ハードウェア記述の自動生成プログラムの作成を行う。最後に、IRF のサイズと、動作周波数、ハードウェア使用量の関係を調べる。

## 3　IRF の動作検証

RISC-V 命令セットを持つ SCR1 プロセッサに IRF を搭載する。SCR1 でフェッチされた命令は、プレデコーダで通常命令か短縮命令かを判断されたあと、デコーダに渡される。そのため、IRF はプレデコーダとデコーダの間に設置する。短縮命令を参照する IRF 命令が通常命令と誤認識されないよう、プレデコーダに変更を施す。動作検証では、一部の命令を IRF 命令に置き換えたプログラムを用意し、IRF 未搭載 SCR1 と IRF 搭載 SCR1 で実行した。結果、IRF 搭載 SCR1 でのみ正常に動作した。

## 4　IRF の自動生成プログラムの動作検証とハードウェア量

ユーザがテキストファイルに変更したい命令を書き、実行すると、その命令に対応した IRF のハードウェア記述が自動生成されるプログラムを作成した。動作検証では、一部の命令を IRF 命令に置き換えたプログラムを用意し、自動生成された IRF を搭載した SCR1 で実行した。命令実行ログ、実行結果を確認すると、命令の置き換え、実行が正常に行われていた。

IRF 命令の数を変化させ、動作周波数、ハードウェア使用量を検証した。結果、動作周波数に大きな変化がないうえ、IRF のハードウェア量はプロセッサ全体のハードウェア量に対し、1% 未満であった。

## 5　結論

本研究では、複数の短縮命令、通常命令に対応した IRF の実装と IRF 自動生成プログラムの作成、命令数とハードウェア使用量の関係の調査を行った。その結果、RISC-V の短縮命令が実行できる RISC-V を搭載している SCR1 において、複数の、かつ通常命令と短縮命令の両方に対応した IRF を実装することができた。また、IRF の自動生成プログラムにより、ユーザがより手軽に任意の命令を IRF 命令に置き換えられるようになった。そして、IRF の搭載による性能やハードウェア量への影響は軽微であることがわかった。

## 参考文献


[1] N. Fujieda, T. Tanaka, S. Ichikawa: Design and Implementation of Instruction Indirection for Embedded Software Obfuscation, Microprocessors and Microsystems, Vol. 45, Part A, pp.115–128 ,2016.

[2] 米澤颯真, 藤枝直輝: 命令レジスタファイルによる RISC-V セキュアプロセッサの検討, 電子情報通信学会 2022 年総合大会, No. D-6-6, 2022.